Como estar em conformidade com a IEC61508 e IEC61511

Raquel Toneto Nunes
raquel.toneto@br.yokogawa.com

YOKOGAWA

Assuntos que serão apresentados

vigilantplant®

- Safety Integrity – O que significa?
- Nossa experiência na implementação do FSM
- Nossa experiência com nossos clientes

Safety Integrity acc. IEC 61508 / 61511

vigilantplant®

- Os três parâmetros que definem o máximo SIL que pode ser atingido

Hardware safety integrity

1. Tolerância a Falha de Hardware dos elementos do SIS (tabelas restrições de arquitetura)
2. PFD_{AVG} (baixa demanda) ou PFH (alta demanda ou modo contínuo) da SIF

Systematic safety integrity (IEC 61508 Ed.2: Systematic Capability)

3. Redução/prevenção de falhas sistemáticas no hard- e software (causado por pessoas e incorporado no SIS)

Falhas Sistemáticas podem ser evitadas / reduzidas aplicando o FSM !

FSM - Functional Safety Management

vigilantplant®

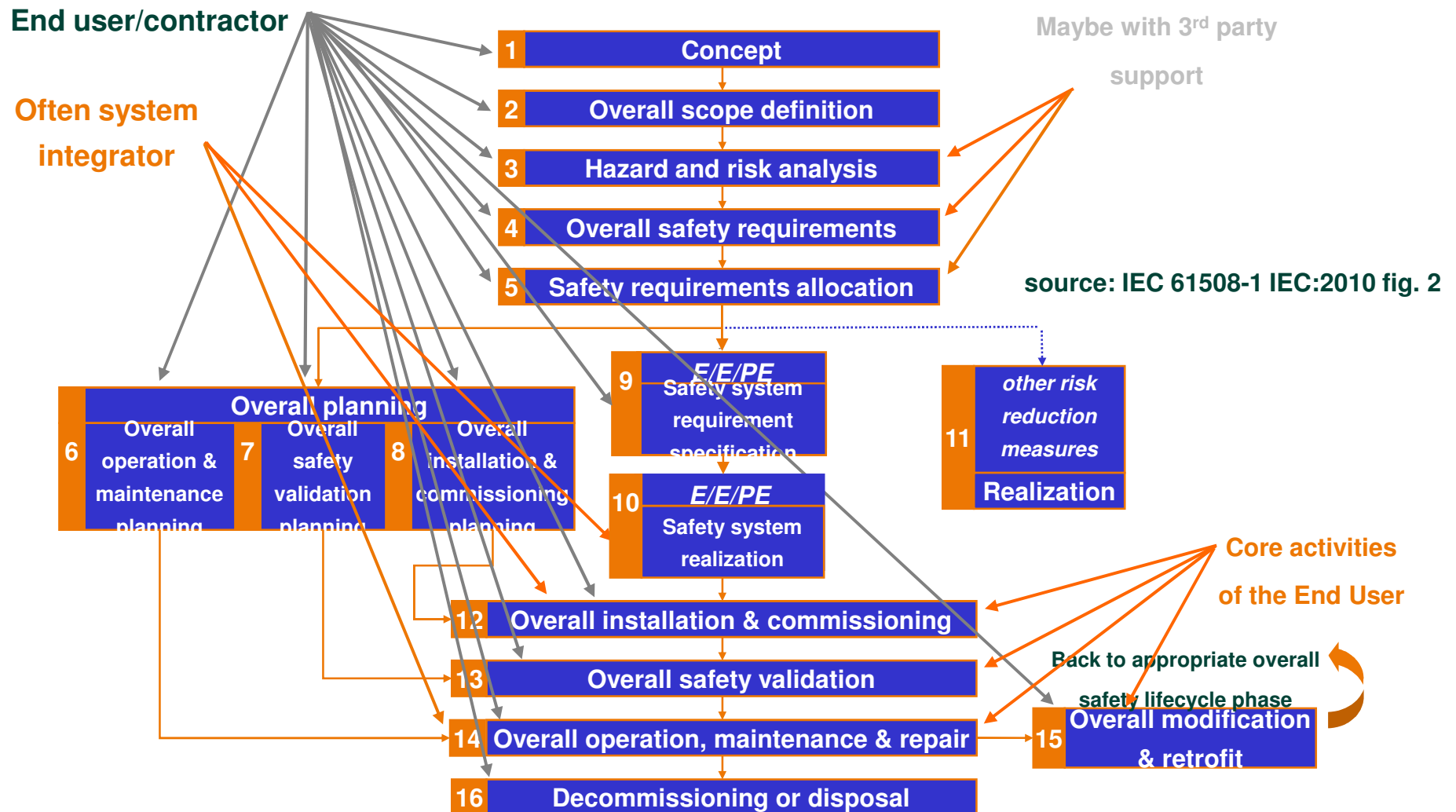
FSM significa:

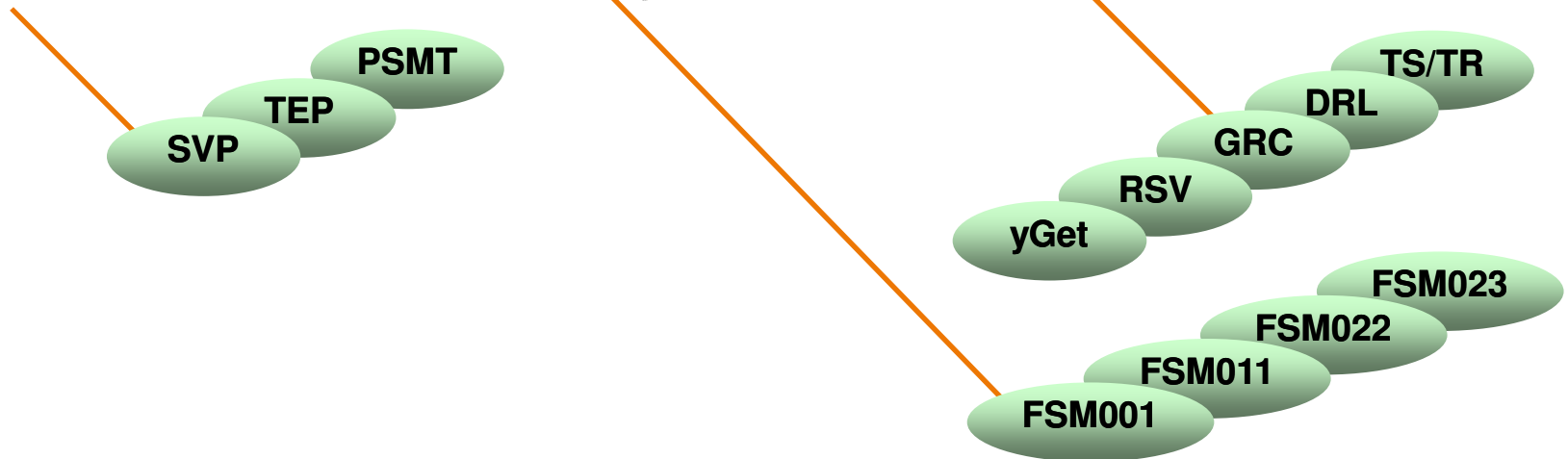
- Ter e usar procedimentos, ferramentas e modelos relacionados a segurança
- Controle de documentos e gerenciamento da configuração (documentação do ciclo de vida, trilha auditável)
- Procedimentos/checklists de revisão e teste (verificação)
- Executar avaliação e validação da seguranaça funcional
- Educar e empregar pessoal competente em seguraça
- Assegurar que a integridade será mantida dentro dos limites do SIL durante todo o tempo de vida do SIS
- Executar auditorias periódicas de segurança
- Executar todos os itens anteriores e documentar o que foi feito!

Safety Lifecycle conforme IEC 61508

vigilantplant.

FSM - Implementação

vigilantplant.®

Primeiro passo: análise de falhas

- **Investigação do Sistema de Qualidade corrente - ISO (2)9001**
- **Definir omissões referentes aos requisitos IEC 61508/61511**
- **Corrigindo as falhas → procedimentos, ferramentas, modelos**

PSMT
TEP
SVP

TS/TR
DRL
GRC
RSV
yGet

FSM023
FSM022
FSM011
FSM001

Conforme IEC 61508

vigilantplant®

- **Lista de Referência Cruzada: Sistema de Qualidade versus requisitos do FSM IEC 61508**

IEC 61508 part	clause	OK		Yokogawa reference
1	5	√		
1	5.2	√		
1	5.2.1	√		PDR
1	5.2.2	√		PDR
1	5.2.3	√		SVP, SAVC
1	5.2.4	√		
1	5.2.5	√		PDR
1	5.2.6	√		PDR
1	5.2.7	√		FSM022
1	5.2.8	√		
1	5.2.9	√		FSM022
1	5.2.10	√		PDR
1	5.2.11	√		PDR
		√		FSM022
1	6	√		
1	6.2	√		
1	6.2.1	√		YQS, SVP
	a	√		FDS, SVP
	b	√		
	c	√		YQS
	d	√		PDR
	e	√		See mentioned sub
	f	√		SVP, SAVC
	g			

Template: Safety Validation Plan

Safety Assessment and Validation Checklist

Procedure: Control of Documents

Project Document Register

Conforme IEC 61511

vigilantplant.®

- **Lista de Referência Cruzada: Sistema de Qualidade versus requisitos do FSM IEC 61511**

IEC 61511 part	clause	OK		Yokogawa reference
1	**5**	√		
1	**5.2**	√		
1	**5.2.1**	√		FSM001
1	5.2.1.1	√		FSM001
1	5.2.1.2	√		FSM001
1	**5.2.2**	√		
1	5.2.2.1	√		Competence/training filed at HRM
1	5.2.2.2	√		Competence/training filed at HRM
1	**5.2.3**	n.a.		Contractor, End User
1	**5.2.4**	√		SVP
1	**5.2.5**	√		
1	5.2.5.1	√		Registration and follow-up via Tracker or punch list
	a)	n.a.		Contractor, End User
	b)	√		FSM011, SAVC, W901_00, F901_03
	c)	√		FSM011, FSM021 and FSM021.01, DRL, TEP, TS/TR
	d)	√		FSM011, SCERT
	e)	√		Contractor, End User
1	5.2.5.2	√		W805_00, F805_01, _02, _03
1	5.2.5.3	n.a.		Contractor, End User
1	**5.2.6**	√		
1	**5.2.6.1**	√		
1	5.2.6.1.1	√		FSM011
1	5.2.6.1.2			
1	5.2.6.1			
	*	√		FSM011
	*	√		Punchlist
	*	√		Validation to

FSM Policy

Template:
Test Execution
Plan

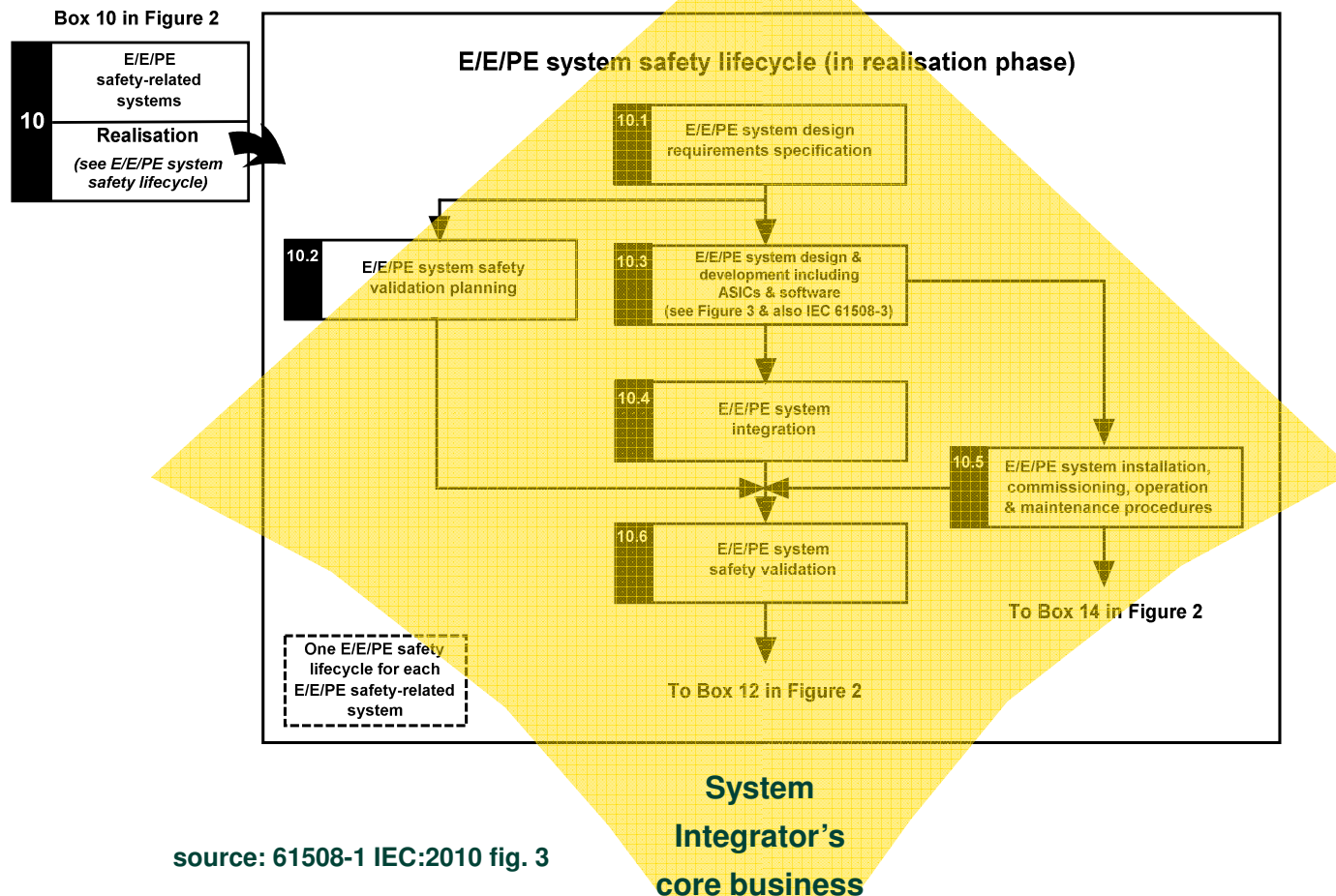
Test Specs
and
Test Records

Not for
Yokogawa

Procedure:
Technical Realization
of
Safety Systems

Fase de Realização

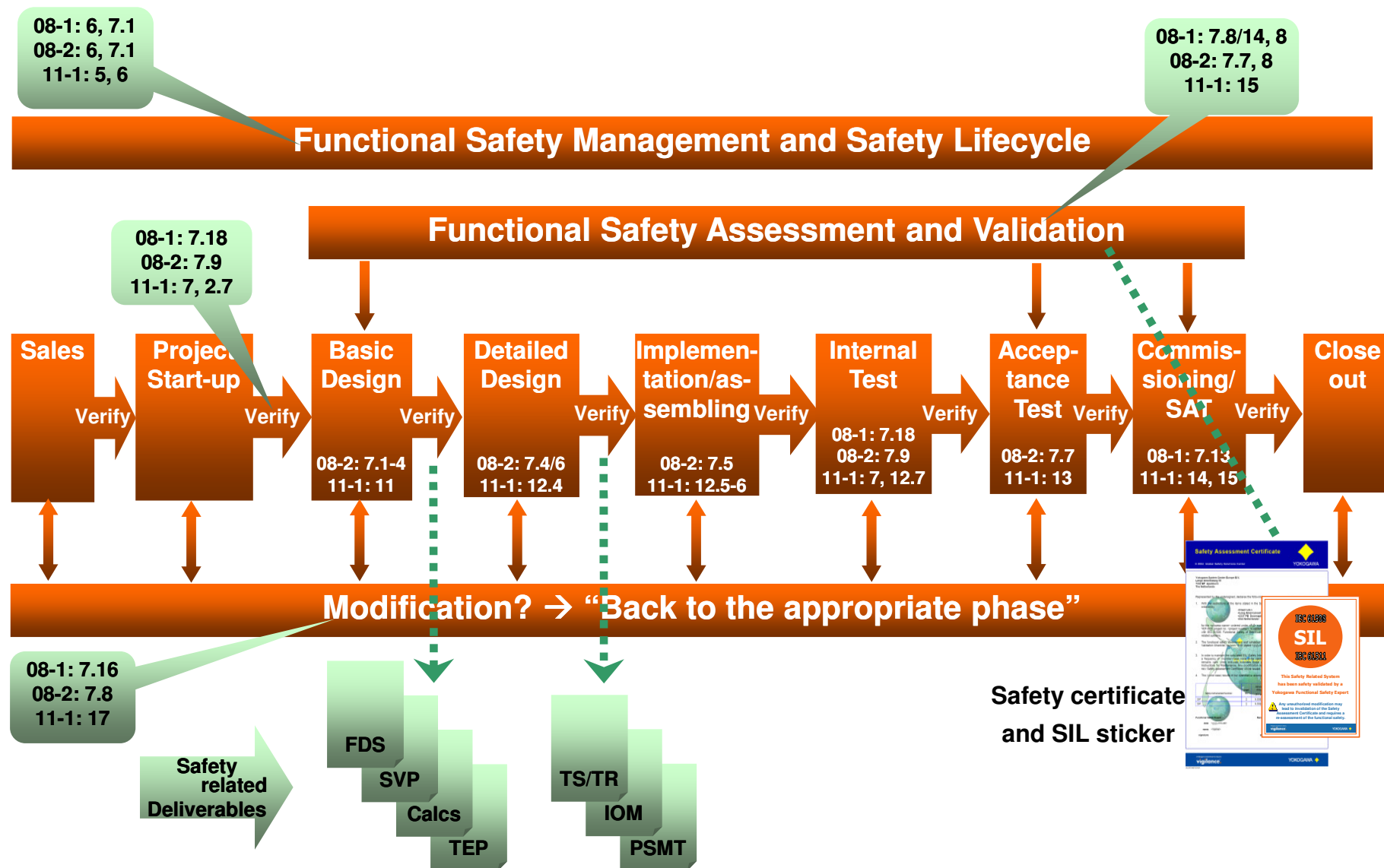
vigilantplant.

- Fase 10 do ciclo-de-vida da IEC 61508

source: 61508-1 IEC:2010 fig. 3

Modelo de Implementação das Fases 10, 12 e 15

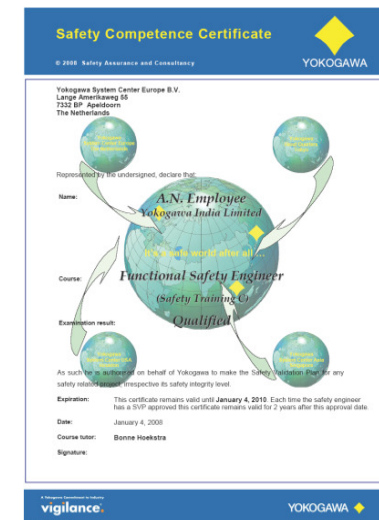
vigilantplant.®

FSM – Competência em Segurança

vigilantplant®

Todos os envolvidos de qualquer forma e em qualquer ponto do ciclo de vida deve ter competência em segurança

O que nós ensinamos aos nosso engenheiros de segurança?

vigilantplant.

- O que Segurança Funcional significa
- Como revisar o SRS?
- Como fazer/reconhecer um projeto de falha segura?
- O que significa redundância em termo de segurança funcional?
- Como executar e registrar revisões detalhadas?
- Como executar e registrar testes detalhados (100%)?
- Nunca revisar ou testar seu próprio trabalho!
- Como calcular o SIL atingido?
- Como lidar com modificações?
- Overrides são aderentes a IEC 61508/61511?
- Como documentar isso tudo?
- Exercitar, exercitar, exercitar

Safety Competence Certificate

FSM – Segurança Funcional Avaliação

vigilantplant®

- Quanto maior o SIL requerido, maior o nível de independência de quem executa a avaliação da segurança funcional
- Executar a avaliação quantitativa bem como qualitativa
- Manter registro dos resultados
- Primeira avaliação durante a fase de basic design
- Avaliação final após o teste de aceitação
- TÜV Rheinland confirmou que a expertise e independência do Yokogawa's SA&C expertise team está aderente a IEC 61508/61511

FSM - Functional Safety Validação

vigilantplant®

Ao final da fase de realização deve ser executada a validação da segurança funcional (sub fase 10.6 da IEC 61508):

- Verificar se todas as verificações (revisões e testes) foram executadas e documentadas
- Testar o (parte do) SIS contra o SRS
- Executar a avaliação final das funções de segurança
- Verificar se todas as pendências relacionadas a seguranaça foram resolvidas
- Verificar se os entregáveis estão completos e atualizados
- Manter registro dos resultados

FSM - Functional Safety Auditoria

vigilantplant.®

- Como a ISO (2)9001 o FSM é um sistema de gerenciamento de qualidade que deve ser auditado periodicamente
- Yokogawa tem o FSM completamente inserido em seu sistema de qualidade ISO (2)9001
- Auditorias periódicas são executadas e documentadas
- Executada por quem tem o nível apropriado de independência
- Algumas afiliadas também são auditadas por um órgão de certificação externo

08-1: 6.2.1

TÜV Rheinland Group

TÜV Rheinland Industrie Service GmbH
Automation, Software and Information Technology
Certification Body for Functional Safety Management-Systems

ZERTIFIKAT
CERTIFICATE

FUNCTIONAL SAFETY MANAGEMENT
- IEC 61508 / IEC 61511 -

No.: 968/FSM 104.03/06

The Company

Yokogawa System Center Europe B.V.
Lange Amerikaweg 55
NL-7332 BP Apeldoorn
The Netherlands

has proven successfully within the scope of an audit that a Functional Safety Management System (FSM-System) has been introduced and applied accordingly.

The objects of the audit are the requirements defined in the basic standards relating to the **Management of Functional Safety**, the **Documentation**, the **Functional Safety Assessment** as well as the **company specific Safety Lifecycle Phases** according to the scope of certification.

The Scope of Certification is:

IEC 61508: **E/E/PE- safety related System Integration**
IEC 61511: **SIS - Integration**

Object of the Scope of Certification is the integration of **E/E/PE-safety related Systems**, **sensors** and actuators respectively SIS and comprises their **configuration**, **application programming**, **assembly**, and **test** as well as **safety loop calculations** for specific industrial safety applications

The audited FSM-System and its involved company departments fulfill the organizational premises for the listed Scope of Certification. This certification does not replace approval or certification for specific E/E/PE-safety related System Integrations.

Validity: until April 2009

Cologne, 2006-06-20

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

Dipl.-Ing. Stephan Häb, Head of Certification Body for FSM-Systems

Updated information of the audited company, as well as for the Certification Procedure and the meaning of the Scope of Certification are published on the homepage (http://www.tuvasi.com) of the Certification Body.

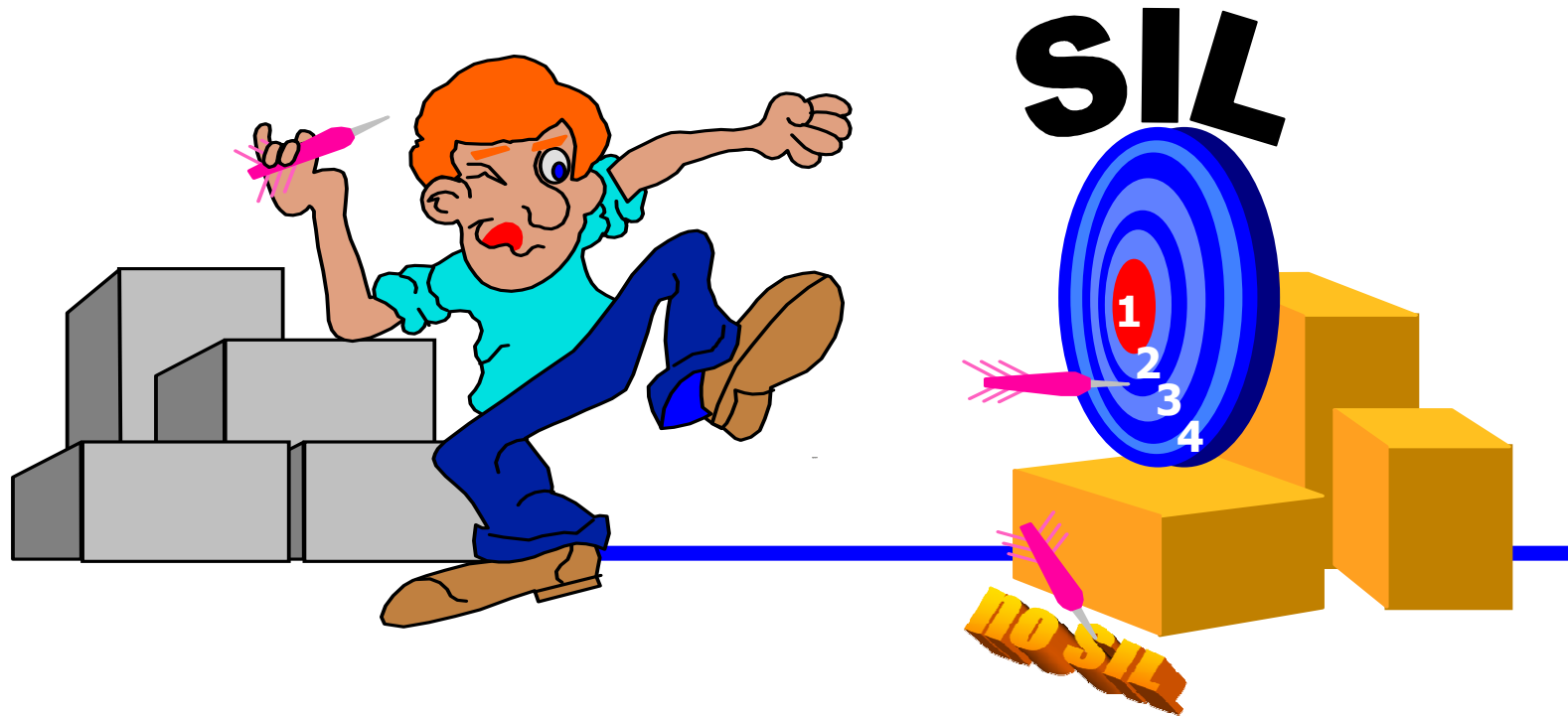
E sobre os nossos clientes?

vigilantplant®

Se os usuários finais se comprometem a aderir a IEC 61508/61511, então eles precisam

- Executar Hazard and Risk Assessments
  - identificar as SIFs
  - determinar o SIL target para cada SIF
- Elaborar o SRS Especificação de Requisitos de Segurança
- Executar Avaliação e Validação de Segurança
- Praticar Operação e Manutenção de Segurança
- Executar e preparar com cuidado as Modificações (análise de impacto)
- Ter e usar um FSM

Definindo o SIL target

vigilantplant.

Nossa estimativa: em >70 % dos casos o usuário final não executa uma avaliação formal de riscos.

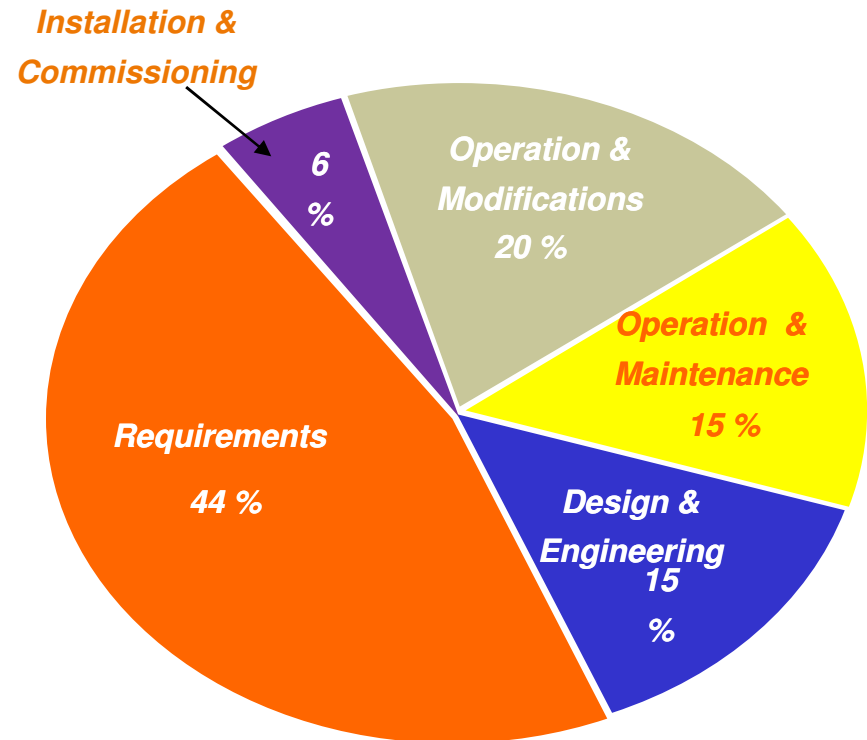
Revendo os Requisitos de Segurança

vigilantplant.

~ 70%:

- Matrizes de Causa e Efeito
- Listas de I/O
- Um requisito de SIL geral

~ 30%:

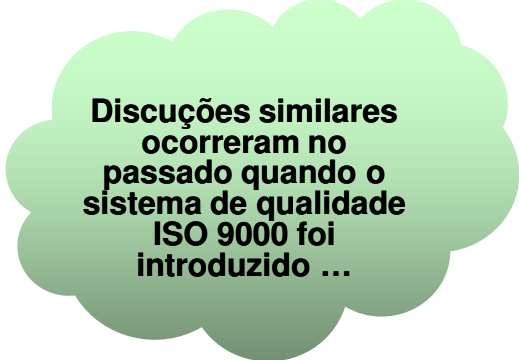
- SIFs definidas
- SIL por SIF

Causes of Systematic Failures
Source: HSE 2004

A boa notícia:

Temos observado uma melhora todos os anos

Segurança, FSM e custos

vigilantplant.

Segurança custa dinheiro?

- A resposta é: inicialmente SEMPRE

Segurança economiza dinheiro?

- A resposta é : a longo prazo SIM

O FSM economiza dinheiro?

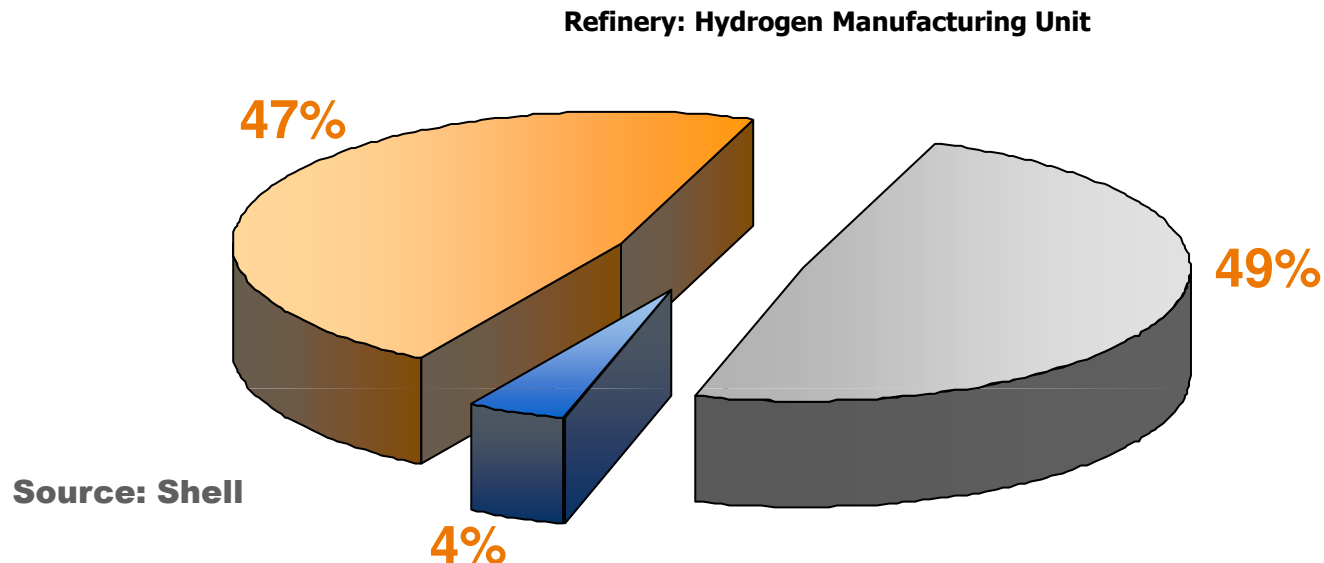
- A resposta é:

  - inicialmente AS VEZES,

  - a longo prazo SEMPRE

Discuções similares ocorreram no passado quando o sistema de qualidade ISO 9000 foi introduzido ...

Avaliação de uma planta, com proteções de segurança antes da introdução da IEC 61511

vigilantplant.®

49%: Funções de Segurança estavam super estimadas

4%: Funções de Segurança estavam subestimadas (inseguras)

47%: Não mudaram

Obrigado!

Departamento de Marketing